



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/750,594	12/31/2003	Ryan Charles Catherman	RPS920030206US1	8589
45503 7590 12/12/2007 DILLON & YUDELL LLP 8911 N. CAPITAL OF TEXAS HWY., SUITE 2110 AUSTIN, TX 78759			EXAMINER PATEL, NIRAV B	
			ART UNIT 2135	PAPER NUMBER
			MAIL DATE 12/12/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

## Office Action Summary

Application No.

10/750,594

Applicant(s)

CATHERMAN ET AL.

Examiner

Nirav Patel

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 21 September 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-8, 10, 11 and 17-24 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☐ Claim(s) 1-8, 10, 11 and 17-24 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                                | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

### DETAILED ACTION

1. This action in responsive to the communication filed on Sep. 21, 2007. Claims 1-8, 10, 11, 17-24 are pending.

2. Applicant's election without traverse of the elected group I, claims 1-8, 10, 11, 17-24, in the reply filed on 9/21/07 is acknowledged. Claim 12, 13, 14, 15 are withdrawn and canceled by the applicant from further consideration pursuant to 37 CFR 1.142(b) as being drawn to a nonelected group II and III, there being no allowable generic or linking claim.

3. The filing of a terminal disclaimer in compliance with 37 CFR 1.321(c) overcomes the double patenting rejection and the rejection is withdrawn.

### Claim Objections

4. Claim 11 is objected to because of the following informalities:

Claim 11 recites "**A TPM device manufactured and authenticated according to the step of claim 1**". The device claim 11 depends on the method claim 1, which is improper form of dependent claim.

Appropriate correction is required.

### Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1-6, 8, 10, 11, 17-22 and 24 rejected under 35 U.S.C. 103(a) as being unpatentable over Challenger (US Pub. No. 2002/0169717) in view of Kean (US Pub. No. 2002/0199110) and in view of Smith (US 6,233,685).

As per claim 1, Challenger teaches:

generating for a valid device an endorsement key pair that includes a private key and a public key (paragraphs 0022-0024, public key, P2, and private key, P4), wherein said private key is not public readable (inherent trait of public/private key pairs); creating a non-public, non-public, secure value (paragraph 0021 and 0024, private key, P3); and inserting an endorsement certificate into said device to indicate that said device is an approved device by an OEM (original equipment manufacturer) of the device (paragraph 0024, certificate, C2).

Kean teaches creating a non-public, secure value that is provided to both a plurality of valid devices and a credential server, wherein the value is a first value that is provided to a first set of said plurality of valid devices and a second set of said plurality of valid devices are provided a second value, based on a pre-defined method for determining when to change said first value to said second value from among: a passage of a pre-set amount of device manufacturing time and a preset number of manufactured devices from among the plurality of valid devices [Fig. 2, paragraph 0012, 0191].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Kean with Challener, since one would have been motivated to prevent reverse engineering and protect confidential information [Kean, paragraph 0028].

Smith teaches, verifying by utilizing said non-public, secure value that an endorsement key of said valid device is a valid endorsement key of said endorsement key pair that was generated during manufacture of said valid device, wherein a function of a first copy of said non-public, secure value within said credential server matches a similar function of a second copy of said non-public, secure value associated with the endorsement key received at the credential server [col. 8 lines 35-67 to col. 9 lines 1-28].

It would have been obvious to one of ordinary skill in the art at the time of invention to combine the method of Challener for generating an endorsement key, creating a signing key, and inserting an endorsement certificate with the method of Smith et al. for verifying that a key is in fact a key from the device in order to certify the device [Smith, col. 8 lines 60-63].

As per claim 2, the rejection of claim 1 is incorporated and Smith teaches:

said non-public, secure value is a secret number and said method further comprises forwarding a first copy of said secret number via a secure communication medium to said credential server [col. 9 lines 12-17].

As per claim 3, the rejection of claim 1 is incorporated and Challenger teaches:

hashing a second copy of said secret number with a public key from said endorsement key pair; combining a first hash result from said hashing step with the public key to create the endorsement key (EK); and forwarding said EK to said credential server to initiate a credential process [paragraph 0023].

As per claim 4, the rejection of claim 1 is incorporated and Challenger teaches:

receiving said EK from said device at the credential server; hashing the public key within the received EK with the first copy of said secret number received during said forwarding step to provide a second hashed value; comparing the first hashed value from within the EK with the second hash value; and confirming said EK is from a valid device when said comparing step results in a match [paragraph 0023].

As per claim 5, the rejection of claim 1 is incorporated and Challenger teaches:

a CA which inherently stores the credential in a database of said credential server; monitors for a request from a customer to provide said certificate to said device (this is done with the request for certification); and following a receipt of said customer request, transmitting said certificate to said device to be inserted within the device (this is done after the certification).

As per claim 6, the rejection of claim 1 is incorporated and Challenger teaches:

It is inherent in TCPA for the endorsement key to be once writable, public readable [see TCPA Spec 1.1b, page 261] therefore it would have been obvious to one of ordinary skill in the art to make the certificate once writable, public readable.

As per claim 8, the rejection of claim 1 is incorporated and Smith teaches:

that the CA can be a remotely located third party with a secure connection [column 8 lines 31-43].

As per claim 10, the rejection of claim 1 is incorporated and Challenger teaches:

creating/manufacturing and authenticating a Trusted Platform Module in the Abstract and paragraph 6.

As per claim 11, the rejection of claim 1 is incorporated and it encompasses limitations that are similar to limitations of claim 1. Thus, it is rejected with the same rationale applied against claim 1 above.

As per claim 17, it encompasses limitations that are similar to limitations of claim 1. Thus, it is rejected with the same rationale applied against claim 1 above.

As per claim 18, the rejection of claim 17 is incorporated and it encompasses limitations that are similar to limitations of claim 2. Thus, it is rejected with the same rationale applied against claim 2 above.

As per claim 19, the rejection of claim 18 is incorporated and it encompasses limitations that are similar to limitations of claim 3. Thus, it is rejected with the same rationale applied against claim 3 above.

As per claim 20, the rejection of claim 19 is incorporated and it encompasses limitations that are similar to limitations of claim 4. Thus, it is rejected with the same rationale applied against claim 4 above.

As per claim 21, the rejection of claim 17 is incorporated and it encompasses limitations that are similar to limitations of claim 5. Thus, it is rejected with the same rationale applied against claim 5 above.

As per claim 22, the rejection of claim 17 is incorporated and it encompasses limitations that are similar to limitations of claim 6. Thus, it is rejected with the same rationale applied against claim 6 above.

As per claim 24, the rejection of claim 17 is incorporated and it encompasses limitations that are similar to limitations of claim 8. Thus, it is rejected with the same rationale applied against claim 8 above.

6. Claims 7 and 23 rejected under 35 U.S.C. 103(a) as being unpatentable over Challenger (US Pub. No. 2002/0169717) in view of Kean (US Pub. No. 2002/0199110) in view of Smith (US 6,233,685) and in view of Wood et al (US Pub. No. 2006/0072747).

As per claim 7, the rejection of claim 1 is incorporated and Wood teaches:

using a temporary key pair [figure 6, step 605-645; paragraphs 36-39] after which the key is no longer used (discarded).

It would have been obvious to one of ordinary skill in the art at the time of invention to combine the method and system of Challenger and Smith et al. with the temporary key of Wood et al. in order to provide additional security [Wood et al, paragraph 0039].

As per claim 23, the rejection of claim 17 is incorporated and it encompasses limitations that are similar to limitations of claim 7. Thus, it is rejected with the same rationale applied against claim 7 above.

### **Response to Amendment**

7. This written action is responding to the communication filed on Sep. 21, 2007. Applicant's amendment filed on June 11, 2007 has been considered. Among the amended claims 1, 17 have been modified to include the limitation from claim 9 and 25 respectively. However, upon further consideration, a new ground(s) of rejection is based on Challenger (US Pub. No. 2002/0169717) in view of Kean (US Pub. No. 2002/0199110) and in view of Smith (US 6,233,685). See new ground of rejection above.

### **Conclusion**

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Lee et al (US 6950941) – Copy protection system for portable storage media

Matsumoto et al (US 6711264) – Security improvement method and security system

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nirav Patel whose telephone number is 571-272-5936. The examiner can normally be reached on 8 am - 4:30 pm (M-F).

Application/Control Number:  
10/750,594  
Art Unit: 2135

Page 10

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

*NBP*

12/8/07



KIM VU

SENIOR PATENT EXAMINER  
ELECTRONIC BUSINESS CENTER 2107